Microsoft

Operating System

End-to-End Security: An Introduction to Internet Protocol Security (IPSec)

Beta 3 Technical Walkthrough

Abstract

Microsoft® Windows® 2000 operating system IPSec provides application-transparent encryption services for network traffic, and other network access protections for the Windows 2000 operating system. Using IPSec, you can provide privacy, integrity and authenticity for network traffic in the following scenarios:

- Provide for end-to-end security from client to server, server to server, and client to client, using IPSec transport mode.
- Secure remote access from client to gateway over the Internet using Layer 2 Tunneling Protocol (L2TP) secured by Internet Protocol Security (IPSec).
- Secure gateway to gateway connections, across outsourced private WAN or Internet-based connections using L2TP/IPSec tunnels, or using pure IPSec tunnel mode.

This walkthrough focuses on the fastest way to use IPSec transport mode to secure application traffic between a client and a server. It demonstrates how to enable security using IPSec default policies between two Windows 2000-based systems that are joined to a Windows 2000 domain. Once you have joined the two computers to the domain, you should complete the first part of the walkthrough, which demonstrates default policies, in 30 minutes or less. Notes are included on how to enable non-IPSec clients to communicate to the server. Steps are provided on how to use certificates, and how to build your own custom policy for further interoperability testing, or to demonstrate IPSec when a Windows 2000 domain is not available.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

0699

CONTENTS

INTRODUCTION

The Microsoft® Windows® 2000 Server operating system simplifies deployment and management of network security with Windows IP Security, a robust implementation of the IP Security Protocol (IPSec). Designed by the Internet Engineering Task Force (IETF) as the security architecture for the Internet Protocol (IP), IPSec defines IP packet formats and related infrastructure to provide end-to-end strong authentication, integrity, anti-replay, and (optionally) confidentiality for network traffic. An on-demand security negotiation and automatic key management service is also provided using the IETF-defined Internet Key Exchange (IKE), RFC 2409. IPSec and related services in Windows 2000 have been jointly developed by Microsoft and Cisco Systems, Inc.

Windows IP Security builds upon the IETF IPSec architecture by integrating with Windows 2000 domains and the Active Directory™ directory services. The Active Directory delivers policy-based, directory-enabled networking using Group Policy to provide IPSec policy assignment and distribution to Windows 2000 domain members. The implementation of IKE provides three IETF standards-based authentication methods to establish trust between computers:

- Kerberos v5.0 authentication provided by the Windows 2000 domain infrastructure, used to deploy secure communications between computers in a domain or across trusted domains.
- Public/Private Key signatures using certificates, compatible with several certificate systems, including Microsoft, Entrust, VeriSign and Netscape.
- Passwords, termed *pre-shared authentication keys*, used strictly for establishing trust.

Once peer computers have authenticated each other, they generate bulk encryption keys for the purpose of encrypting application data. These keys are known only to the two computers. So their data is very well protected against modification or interpretation by attackers who may be in the network. Each peer uses IKE to negotiate what type and strength of keys to use, as well as what type of security with which to protect the application traffic. These keys are automatically refreshed according to IPSec policy settings to provide constant protection under the administrator's control.

Scenarios for Using IPSec End-to-End

Internet Protocol Security (IPSec) in Windows 2000 is designed to be deployed by network and system administrators so that users' application data can be transparently secured. It is critical that you perform tests with Windows 2000 Beta 3, using real scenarios and real applications (as they exist on your network) as much as possible. In all cases, using Kerberos authentication and domain trusts is the easiest choice for deployment. Certificates or pre-shared keys can be used for untrusted domain or third- party interoperability as necessary. You can use Group Policy to deliver the IPSec configuration, called an *IPSec policy*, to many clients and servers.

Secure Server

IPSec security for all traffic is either requested but optional, or requested and required by the administrator's configuration of the server. Clients need only a default policy for how to respond to security requests from servers.

Secure Applications

Security for applications can be achieved in two ways. First, the servers hosting the applications can be secured so that the clients only use their response capability as above. This is the easiest approach to take, and can be done safely as long as the application's first packets sent to the server do not contain sensitive data. If the first packets do contain sensitive data, then the client must receive an IPSec policy to request security for traffic when it attempts to send data to the specific application servers.

Second, clients and servers can have specific rules for securing certain network packets (protocol or port specific). This approach is more difficult to configure and prone to error because it requires in-depth knowledge of the type of network traffic that an application sends and receives, and administrative coordination to be sure that all clients and servers have compatible policy.

Additional Reference Information

The Windows 2000 Server online help contains basic and more extensive discussions of IPSec functionality than this walkthrough. To access the online help for Windows 2000 Professional and Server, use the procedures in the walkthrough to run the IPSec Policy Management tool, and then choose Help.

Information about Microsoft's support for Virtual Private Networking can be found in the white paper available at: http://www.microsoft.com/ntserver/commserv/

Detailed information on IPSec in Windows® 2000 Beta3 can be found in the Beta3 release notes addendum available at:
http://ntbeta.microsoft.com/documentation/relnotestoc.asp

For the latest information on Windows 2000, check the Microsoft Web site at http://www.microsoft.com/windows and the Windows NT Server Forum on the Microsoft Network (GO WORD: MSNTS). Other Windows 2000 Beta 3 walkthroughs and technical information are available at:

http://www.microsoft.com/windows/server/default.asp
If you are already a technical beta site, then you have an account for access to the site: http://ntbeta.microsoft.com

The IETF specifications relating to IPSec are at:
http://www.ietf.org/html.charters/ipsec-charter.html

BEFORE YOU BEGIN

Pre-requisites

This walkthrough is designed as a lab for network and system administrators. You can work with a partner to configure an IP security policy locally on each computer. You and your partner will implement this policy and test the results of the policy to see secure network communications. If you do not have a partner, then perform the partner steps on the second computer yourself.

To complete this walkthrough, you need the following:

- Two computers running Windows 2000 Beta 3. (You may use two Windows 2000 Professional systems as the domain members, one to act as a client and the other as a server in the IPSec sense.)
- A Windows 2000 Server to be the domain controller.
- The three computers must be connected by a local or wide area network.
- The two test systems must be joined as a member of the same (or a trusted) domain.

If you have a Kerberos v5 server and wish to test interoperability with it, please refer to the walkthrough on how to configure that scenario.

You can also use IP Security without the two computers being domain members. To achieve this, please see the section on building a custom policy. You must have two domain members to use the built-in policies, because they require Kerberos authentication provided by the domain controller.

After completing this walkthrough, you will be able to:

- Use a built-in IPSec policy.
- Create your own IPSec policy.
- Check the status of IP Security.

Collecting Information

You will need the following information to complete this walkthrough, and might find it useful to note it down here:

Your Host Name: _____

Your IP Address: _____

Complete the information below.

Partners Host Name: _____

Partners IP Address: _____

It's also a good idea to start and minimize a Command Prompt window for later use.

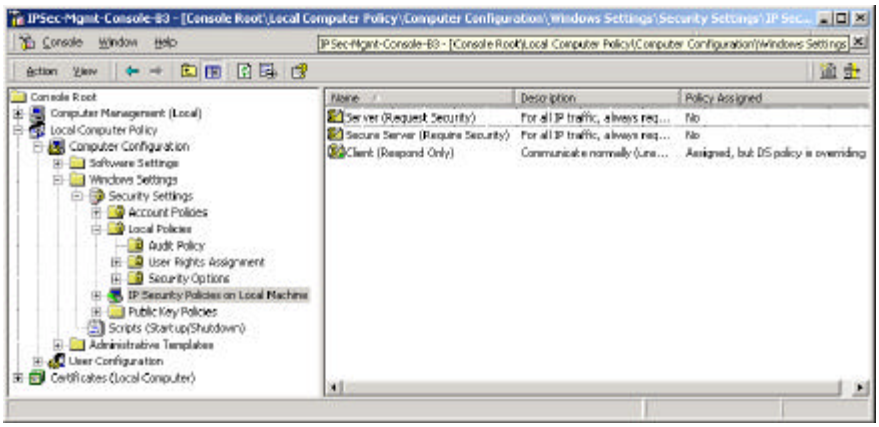
Creating a Custom Console

First, you need to create a custom Microsoft Management Console (MMC).

To construct a custom MMC console for your work

1. On the **Start menu**, click **Run**, and in the Open text box, type **mmc**, and then click **OK**.
2. On the Console menu, click **Add/Remove Snap-in**.
3. In the **Add/Remove Snap-in** dialog box, click **Add**.
4. In the **Add Standalone Snap-in** dialog box, click **Computer Management**, and then click **Add**.
5. Verify that **Local Computer** is selected, and click **Finish**.
6. In the **Add Standalone Snap-in** dialog box, click **Group Policy**, and then click **Add**.
7. Verify that **Local Computer** is selected in the **Group Policy** Object dialog box, and click **Finish**.
8. In the **Add Standalone Snap-in** dialog box, click **Certificates**, and then click **Add**.
9. Select **Computer Account**, and click **Next**.
10. Verify that **Local Computer** is selected, and click **Finish**.
11. To close the **Add Standalone Snap-in** dialog box, click **Close**.
12. To close the **Add/Remove Snap-in** dialog box, click **OK**.

The Microsoft Management Console consists of two panes, a scope pane on the left, consisting of Computer Management, Local Computer Policy and Certificates (Local Computer), and a results pane on the right.



Note This is a general console for IPSec management and will be used in other walkthroughs. Some of the snap-in features will not be used in this particular walkthrough.

Enabling Audit Policy for Your Computer

In the next step, you will configure auditing, so that an event will be logged when IPSec comes into play. Later, this will be a useful confirmation that IPSec is working properly. To configure auditing, execute the following steps on both of the computers you are using for this walkthrough.

To enable audit policy

1. In the **MMC console** that you created earlier, select **Local Computer Policy** from the scope pane of the **MMC**, and click **+** to expand the tree. Then navigate to **Computer Configuration**, to **Windows Settings**, to **Security Settings**, then to **Local Policies**, and select **Audit Policy**.
2. From the list of **Attributes** displayed in the results pane, double-click **Audit Logon Events**. The **Audit Logon Events** dialog box appears.
3. In the **Audit Logon Events** dialog box, click to select the **Audit successful attempts** and **Audit failed attempts** check boxes, and click **OK**.
4. Do the same for the **Audit Object Access** attribute.

Configuring the IP Security Monitor

To monitor the successful security connections that the IPSec policy will create, you use the IP Security Monitor tool. Before creating any policies, first start and configure the tool.

To start and configure the IP Security Monitor

1. Start the IP Security Monitor tool: click **Start**, then click **Run**, and type **ipsecmon** into the Open box. Click **OK**.
2. Click **Options** in the IP Security Monitor tool, and change the default value for **Refresh Seconds** from 15 to 5 or 1. Click **OK** to return to the tool.
3. Minimize the IP Security Monitor window.

You will use this minimized tool to monitor the policies later in this walkthrough.

USING A BUILT-IN IP SECURITY POLICY

In this exercise, you will activate one of the built-in IPSec policies to secure traffic between the two computers. The default policies use Kerberos as the initial authentication method. Because both machines are members of a Windows 2000 domain, a minimal amount of configuration is required.

To activate the policy

1. In the **MMC** console you created earlier, select **IP Security Policies on Local Machine** from the scope pane. There are three entries in the results pane, **Server, Secure Server**, and **Client**.
2. On one computer, right-click **Secure Server**, and then choose **Assign**. The status in the **Policy Assigned** column should change from **No** to **Yes**.
3. On the other computer, right-click **Client**, and then choose **Assign**.

   Now you have one computer acting as a client and the other as a secure server. The client will send initial ping (ping is an application of Internet Control Message Protocol, or ICMP) packets (and any other traffic to other destinations) unprotected to the server, but the server will request security from the client and the rest of the communication will be secure. If the server were to initiate the ping, then the ping would have to be secured to the client before the server would allow it on the network. If the client computer also had a secure server policy as well, then it would not send traffic unprotected pings or any other traffic, rather it would request IPSec protection before any application data is sent on the network. If both computers had client policies, no data would be protected, because neither side requests security.

   Note Wait until your partner completes this procedure on his or her computer**.**
4. Open a **Command Prompt** window on the computer that has the client IPSec policy, and type **ping partners-ip-address**. You should receive two to four **Request Timed Out** responses, because the client is not initiating IPSec security (the IKE negotiation). It is only sending ping traffic in the clear.
5. Restore the **IP Security Monitor** window, which you minimized earlier. You should see details of the Security Association that is currently in use between your two machines, as well as statistics on the number of Authenticated and Confidential bytes transmitted.
6. Repeat the ping command, and you should receive four successful replies now that the two computers have established IPSec security associations between them.
7. On the computer that initiated the ping, from the scope pane in the **MMC**, select **Computer Management**, Navigate to **System Tools,** to **Event Viewer,** and then to **Security Log**. In Security Log, you should see Logon audit event 541, noting the successful establishment of an IPSec security association (SA):

```
ISAKMP security association established
Peer Identity:

Kerberos based Identity: machine$@domainname
Peer IP Address: <ping responder IP address>

 Filter:
Source IP Address <ping initiator IP address>
Source IP Address Mask 255.255.255.255
Destination IP Address <ping responder IP address>
Destination IP Address Mask 255.255.255.255
Protocol 0
Source Port 0
Destination Port 0

 Parameters:

ESP Algorithm DES
HMAC Algorithm MD5
AH Algorithm None
Encapsulation Transport Mode
InboundSpi <a large number>
OutBountSpi <a large number>
```

Note that the SPI numbers may appear negative. This is a known bug and will be fixed post Beta 3. The algorithm information may vary, and can be varied by editing the policy defaults, depending on the specific configuration you are testing. Microsoft recommends that you do not change the defaults, but rather create a new policy for testing other configurations.

You have successfully configured and used IP Security between the two computers.

Impact of Secure Server Policy on a Computer

Only IPSec clients that can successfully negotiate will be able to communicate with the secure server computer. Also, the secure server will not be able to talk to other systems, such as Domain Name System (DNS), unless that traffic can be secured using IPSec. Because many services are running in the background on the server, they will probably fail to communicate and generated event log messages. This is normal, because the default Secure Server policy is very severe and attempts to secure almost all IP packets before letting them into the network.

Allowing Non-IPSec Clients To Talk with A Server

To allow non-IPSec clients to communicate as well, you should assign the **Server** policy, instead of **Secure Server**. This will always request security, but will allow unsecured communication with clients, by falling back to clear text if the client does not reply to the IKE negotiation request. If at any time the client does reply, then a negotiation is in progress and must succeed completely. If negotiation fails the communication will be blocked for one minute, whereupon another negotiation will be attempted. See the section, “Configuring an IPSec Filter Action,” for more explanation on the settings that are used to control this behavior.

Unassign the **Secure Server or Server** and **Client** policies to return your computers to their previous states, by right-clicking the policy, and then clicking **Unassign** .

BUILDING A CUSTOM IPSEC POLICY

In the previous section, you used one of the built in IPSec policies to secure traffic between two domain members. If you want to secure traffic between two computers that aren't domain members, you need to create a custom policy because the built-in policies require Kerberos authentication provided by the domain controller. There are other reasons for creating a custom policy, for example if you wanted to secure traffic based on network address. In this section, you will create a custom IPSec policy, first by defining a security rule, then by defining a filter list, then finally by specifying the filter action.

Configuring an IPSec Policy

Before configuring the IPSec Authentication Method, Filter List or Negotiation method, you must first create a new policy.

To create an IPSec Policy

1. In the scope pane of the **Microsoft Management Console**, right-click **IP Security Policies on Local Machine**, and then click **Create IP Security Policy**. The IP Security Policy Wizard appears.
2. Click **Next**.
3. Type **Partner** as the name of your policy, and click **Next**.
4. Clear the **Activate the default response rule** check box, and then click **Next**.
5. Click to select the **Edit Properties** check box, and then click **Finish**.
6. In the **Properties** dialog box for the policy you have just created, ensure that **Use Add Wizard** is checked, and then click **Add** to start the Security Rule Wizard.

The next step in configuring an IP Security Policy is creating an IPSec security rule.

To configure an IPSec Security Rule

1. Click **Next** to proceed through the **Security Rule Wizard**, which you started at the end of the previous section.
2. Choose **This rule does not specify a tunnel**, and then click **Next**.
3. Select the appropriate option to apply this rule to all network connections, and click **Next**.

Configuring an IKE Authentication Method

Here you specify how the computers will trust each other, by specifying how they will authenticate themselves, or prove their identities to each other when trying to establish a security association. IKE for Windows 2000 provides three authentication methods to establish trust between computers:

- Kerberos v5.0 authentication provided by the Windows 2000 domain that serves as a Kerberos v5.0 Key Distribution Center (KDC). This provides easy deployment of secure communications between Windows 2000 computers who

are members in a domain or across trusted domains. IKE only uses the authentication properties of Kerberos. Key generation for IPSec security associations is done using IKE RFC2409 methods. This is documented in draft-ietf-ipsec-isakmp-gss-auth-02.txt.

- Public/Private key signatures using certificates, compatible with several certificate systems, including Microsoft, Entrust, VeriSign, and Netscape.
- Pre-shared Key, which is a password used strictly for establishing trust between computers.

In this exercise, you will use pre-shared key authentication. This is a text word or phrase that both computers, the sender and the receiver, must know in order to be trusted by each other. Both sides of the IPSec communication must know this value. It is not used to encrypt the application data. Rather, it is only used during negotiation to establish whether the two computers will trust each other. The IKE negotiation uses this value, but does not pass it across the network. However, the authentication key is stored in plain text form within the IPSec policy. Anyone with administrative access to the computer (or any valid domain user id for a computer that is a member of the domain where the IPSec policy is stored in the Active Directory) can see the authentication key value. Therefore, Microsoft does not recommend use of pre-shared key for IPSec authentication unless testing or in cases where it is required for interoperability with third party vendor IPSec implementations. Instead, Microsoft recommends using either Kerberos or certificate authentication instead.

To configure the Authentication method for the rule

1. Choose **Use this string to protect this key exchange** and enter ABC123 as the string. You must not use a blank string.
2. Click **Next**. After reading the following description of IPSec filters, you will proceed to create a filter for your policy.

   Note If you want to use certificates for authentication, see the instructions for obtaining a certificate for testing from Microsoft using the Internet available certificate servers.

Configuring an IPSec Filter List

IP Security is applied to IP packets as they are sent and received. Packets are matched against filters when being sent (outbound) to see if they should be secured, blocked or passed through in clear text. Packets are also matched when received (inbound) to see if they should have been secured, should be blocked, or should be passed through (permitted) into the system. A few types of IP traffic cannot be secured by the design of IPSec in Windows 2000:

- Broadcast—addresses usually ending with .255 with appropriate subnet masks[1]
- Multicast—addresses from 224.0.0.0 through 239.255.255.255

[1] See p.171 of TCP/IP Illustrated, Volume 1 The Protocols by W. Richard Stevens for full discussion on what constitutes a broadcast address.

- RSVP—IP protocol type 46
- Kerberos—UDP source and dest port 88
- IKE—UDP dest port 500
- LDAP—UDP source and dest port 389

Individual filter specifications are grouped into a filter list to enable complex patterns of traffic to be grouped and managed as one named filter list, such as "Building 7 File Servers", or "All blocked traffic". Filter lists can be shared as necessary between different IPSec rules in the same policy or different IPSec policies.

When configuring IP Filters for traffic that must be secured, always be sure to mirror the filters. Mirroring filters automatically configures both inbound and outbound filters.

You will be configuring filters between your computer and your partner's computer. You must configure an outbound filter specifying your IP address as the source address and your partner as the destination address. Then the mirror processing will automatically configure an inbound filter specifying your partner's computer as the source address, and your computer's IP address as the destination. In this simple case, there will be only one mirrored filter specification in the filter list.

The same filter list will need to be defined on both computers.

To configure an IP Filter List

1. In the **IP Filter List** dialog box, click **Add**. An empty list of IP filters is displayed. Name your filter **Partner Filter**.
2. Click to select the **Use Add Wizard**, and then click **Add**. This starts the **IP Filter Wizard**.
3. Click **Next** to continue.
4. Accept **My IP Address** as the default source address by clicking **Next**.
5. Choose **A Specific IP address** from the drop-down list box, enter your ***Partners IP Address***, and then click **Next**.
6. Click **Next** to accept the protocol type of **Any**.
7. Click to clear the **Edit Properties** check box, and click then **Finish**.
8. Click **Close** to leave the **IP Filter List** dialog box, and return to the **New Rule Wizard**.
9. In the **IP Filter List** dialog box, click **Partner Filter**, and then click **Next**.

After reading the following section, you can proceed to configure the filter action.

Configuring an IPSec Filter Action

You have just configured both the input and output filters for matching TCP/IP packets. The second step is to configure the action to take for those packets. You can permit, block or secure the packets that match the filters. If you want to secure the traffic, both computers must have a *compatible* negotiation policy configured.

The built-in defaults should serve well for trying out different features. If you want to experiment with specific capabilities, you should create your own new filter action.

Two methods allow communication with computers that are not able to do IPSec:

- Use the filter action of permit to let the packets go in the clear, or unsecured. Use this action in combination with a filter that matches the traffic you want to permit in its own rule within the IPSec policy. Typical uses would be to permit traffic types of ICMP, DNS, or SNMP, or to permit traffic to certain destinations, such as the default gateway, DHCP & DNS servers, or other non-IPSec systems.
- Configure your filter action to use the setting **Fall back to unsecured communication**. You will see this option presented in the wizard. Choosing this option in the wizard will enable (check) the filter action parameter **Allow unsecured communication with non-IPSec aware computer**. Using this setting allows unsecured communication with a destination, by falling back to clear text if the destination does not reply to the IKE negotiation request. If at any time the client does reply, then a negotiation is in progress and must succeed completely. If negotiation fails, the outbound packets that matched the filter will be discarded (blocked) for one minute, whereupon another outbound packet will cause another IKE negotiation to be attempted. This setting only affects IKE negotiations that are initiated by the computer. It has no effect on computers that receive a request and thus respond. The IKE RFC 2409 standard does not provide a method for both sides to negotiate to normal, or unsecured, or clear text mode.

To configure the filter action

1. In the **Filter** dialog box, click to select the **Use AddWizard** check box, and then click **Add**.
2. Click **Next** to proceed through the **Filter Action Wizard**.
3. Name this filter action **Partner Filter Action**, and click **Next**.
4. In the **Filter Action General Options** dialog box, select Negotiate Security, and then click **Next**.
5. Click **Do not communicate with computers that do not support IPSec** from the next wizard page, and then click Next.
6. Select **Medium** from the list of security methods, and click **Next**.
7. Click to clear the **Edit Properties** check box, and then click **Finish** to close this wizard.
8. In the **Filter Action** dialog box, click **Partner Filter Action**, and then click **Next**.
9. Click to clear the **Edit properties** checkbox is, and then click **Close**.

   You have just configured the filter action that will be used during negotiations with your partner. Note that you can re-use this filter action in other policies.
10. In the **Properties** page that is now displayed, click **Finish**. You have successfully configured an IPSec Policy.

    Note Wait here until your partner completes this procedure on his or her computer.

TESTING YOUR CUSTOM IPSEC POLICY

To test your IPSec policy

1. In the MMC console scope pane, select **IP Security Policies on Local Machine**. Note that Partner (the policy you just configured) is in the results pane, in addition to the three built-in policies.
2. Right-click **Partner**, and then click **Assign** from the context menu. The status in the **Policy Assigned** column should change from **No** to **Yes**.
3. Open a command prompt window, and type **ping partners-ip-address**. You should receive four Negotiating IP Security responses. Repeat the command, and you should receive four replies.
4. Restore the IP Security Monitor window (which you minimized earlier). You should see details of the Security Association that is currently in use between your two computers, as well as statistics on the number of Authenticated and Confidential bytes transmitted among others.
5. In the scope pane of the MMC console, select **Computer Management**, and navigate to **System Tools**, to **Event Viewer**, and then select **Security Log**. In the security log, you should see event 541 noting the establishment of an IPSec security association (SA).
6. Repeat step three to unassign the Partner policy, and return your computers to their previous states. This time, when you right-click the policy, click **Unassign**.

USING CERTIFICATE AUTHENTICATION (ADVANCED USERS)

Obtaining a Microsoft Certificate for Testing

You must first obtain a valid certificate to identify the computer from a certificate server. Even if you have another certificate server you want to use, please obtain a Microsoft certificate first for testing. Any valid computer certificate can be used. We have tested compatibility with several certificate systems, including Microsoft, Entrust, VeriSign, and Netscape.

Note Not all certificate servers will automatically enroll your computer and issue a certificate. The certificate must appear in the local computer account under personal certificates and have the Certificate Authority (CA) root in the Trusted Root store. Consult the certificate server walkthroughs for more information on how to obtain certificates from non-Microsoft certificate servers.

To obtain a certificate

1. Open **Internet Explorer** and go to the site **http://sectestca1.rte.microsoft.com**

   This site provides access to four certificate authorities. For simplicity, this procedure uses a certificate issued from the stand-alone CA, sectestca3.

2. Select **Standalone Root (RSA 2048)**.
3. Select **Request a Certificate**, and then click **Next**.
4. Select **Advanced Request**, and then click **Next**.
5. Select **Submit a Certificate Request Using a Form**.
6. In the **Advanced Certificate Request** form, enter the following responses:

   Identifying Information: as desired.

   Extended Key Usage: Client Authentication or Server Authentication.

   There is also an “IPSec Authentication” type of extended key usage to support the specification that is still being developed by the standards groups. You can use this type if you want to inter-operate with other IPSec implementations that require it. However, the default setting for IPSec certificate authentication is to use any valid certificate, meaning any setting of extended key usage.

   Cryptographic Service Provider: Microsoft Base Cryptographic Provider v1.0

   Key Size: 1024

   If you choose a higher key size, the enrollment request may fail because the version of Windows 2000 you are using must adhere to export restrictions.

   Key Spec: Exchange.

   Note This setting determines what the private key can be used to do—encryption of data (or other symmetric encryption key), or signatures only. The current implementation of IKE uses only private keys for signatures. However, future IKE implementations may support additional negotiation options that use the private key for encryption of data in the IKE exchange. Large-scale deployment of certificates that are signature-only may start failing negotiations

that previously worked if such an updated IKE implementation is used.

Hash Algorithm: SHA1/RSA

Additional Options: Use local machine store.

7. Submit the request and install the certificate.
8. Open the **IPSec Management MMC** console to which you added a snap-in to manage Certificates (Local Computer).
9. Verify the certificate enrollment succeeded:
   - The Personal Certificates folder should contain the computer's certificate name that you selected for **<your name> IPSec testing**.
   - Double-click **Personal Certificate** to see the bottom of the General tab. It should contain the message, “You have a private key that corresponds to this certificate”. Note the name of the CA where it says “Issued by:”
   - View the Trusted Root Certificate Authorities, Certificates folder. You should find a certificate in this store with the name of the Issued By certificate authority. You should not have a private key that corresponds to this certificate.

Note If a certificate was obtained from the Microsoft Certificate Server with the option set for *strong private key protection*, a user must enter a PIN number to access the private key each time that the private key is used to sign data in the IKE negotiation. Because the IKE negotiation is being done in the background by a system service, there is no window available to the service to prompt the user. So certificates obtained with this option will not work for IKE authentication.

Tightening Security for Trusted Root Certificate Authorities Store

While you are here, consider what certificate authorities you want your computer to trust. In the next section, you will specify a trusted root certificate authority (CA). A known issue with Windows 2000 Beta 3 may prevent this computer from using L2TP/IPSec until the number of roots in the root store is reduced. If this computer is being used as an L2TP/IPSec VPN server or client, you may need to delete some root certificates, because there are too many to fit in an IKE negotiation packet.

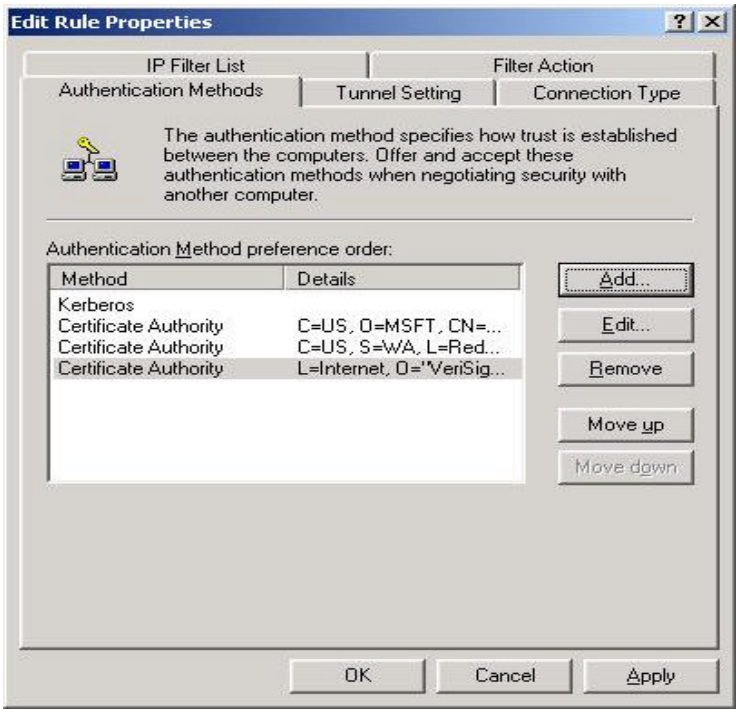
Configuring Certificate Authentication for a Rule

If you are creating a new rule, the wizard will allow you to browse for a certificate authority to use. This is a list of certificate authority certificates that are in the computer trust CA root store, not a list of your personal certificates. This CA specification serves two purposes. First it provides IKE with a CA name that it trusts. Your computer will send a request for a valid certificate from this CA to the other computer. Second, the CA specification provides the name of the CA that your computer will use to look for its own certificate to offer in response to a request.

Caution: You must select the certificate authority that issued your computer a certificate.

If you started the **New Rule Wizard**, then you will be able to select only one CA. If you need to select more, then you can do this through the **IPSec Rule editor** after you complete the wizard.

The IPSec Rule editor allows you to build an ordered list of certificate authorities that your computer will send in a request to the peer computer during IKE negotiation. The peer computer must have a personal certificate issued by one of the CAs in your list in order for the authentication to succeed.



You can continue to add and arrange certificate authorities as you wish.

You can order the list of authentication methods to specify certificates first, then Kerberos or pre-shared key. However, you cannot break up the list of certificates by adding a non-certificate method in the middle.

By adding additional CAs, you are able to build a list of CAs that you trust, which is a greater list than the one (or few) that have issued your computer a certificate. This is necessary for interoperability in many enterprise scenarios.

It is important to understand that your computer may receive certificate requests from a destination that may or may not include a CA in the list of certificates you have specified in policy. Coordination with the administrator of the destination is required to agree on which CAs each side will be using.

- If the destination's request to you does include a certificate authority in this list, then IKE will check to see if your computer has a valid personal certificate from this CA. If you do, then it will choose the first valid personal certificate it finds and send that as the computer's identity.

- If your computer receives a certificate request for a CA that was not specified in this IPSec policy rule, then your computer will send the first certificate it finds that was issued by the CA name that is specified in its policy. Because certificate requests are optional in the RFC 2409 standard, once your computer agrees to certificate authentication, your computer must send a certificate even if it did not receive a certificate request, or if the certificate request yielded no match with your computer's CA names in policy. In this case, it is likely that the IKE negotiation will fail because the two computers could not agree on a common trusted CA. If the destination's request to you does not include one of the certificate authorities here, then the IKE negotiation will fail.

Certificate Revocation List Checking

Most certificate servers issue certificates that contain a Certificate Revocation List (CRL) Distribution Point (sometimes wholly abbreviated as CDP). In order for a computer to validate a certificate completely, it must check to see that the certificate has not been revoked by the issuer. Since the standards for making this check have been evolving, and various certificate servers and PKI systems are already in use, not all of the certificate systems support the same method and functionality of CRL checking. Therefore CRL checking is disabled by default. Before enabling CRL checking, make sure you are successfully authenticating using certificates, and you have examined the Oakley.log trace file to see how the log shows this.

IKE uses the Cryptographic API version 2.0 (CAPIv2) functionality of Windows 2000 for processing certificates. IKE specifies to CAPIv2 how to handle CRL checking when it requests a certificate to be validated. To enable CRL checking, the computer administrator must change the value of the registry key below. The proper setting of this value should be determined by the IPSec policy administrator, and the certificate server administrator.

To enable CRL checking

1. On the **Start** menu, click **Run**, and enter **regedt32**. This starts the Registry Editor.
2. Go to the key

   HKEY_LOCAL_MACHINE\
   \System
   \CurrentControlSet
   \Services
   \PolicyAgent
3. Double-click **Policyagent**.
4. On the **Edit** menu, click **Add Key**.
5. Enter the **Key Name** (case sensitive): **Oakley**.
6. Leave **Class** blank, and click **OK**.
7. Select the new key, **Oakley**.

8. On the **Edit** menu, click **Add Value**.
9. Enter the **Value Name** (case sensitive): **StrongCrlCheck**
10. Select Data Type: **REG_DWORD**, and click **OK**.
11. Enter the value, either **1** or **2**, according to the behavior you want to enable:
    - Use **1** to fail only if CRL check returns that the cert has been revoked (the normal form of CRL checking).
    - Use **2** to fail on any CRL check error. This is the strongest form, and is used when the CRL distribution point must be reachable on the network, and must not say that it never issued the certificate or provide any other error. Effectively, a certificate will pass this level of check only if the CRL processing can positively conclude that certificate is not revoked.
12. Exit from the Registry Editor.
13. Open a command window, and run **net stop policyagent**, then **net start policyagent** to restart the IPSec related services. Or reboot entirely if your system in configured as a VPN server for L2TP/IPSec.

Much more detail is available regarding how CAPI does certificate revocation checking in the Windows 2000 resource kit, and in the online help for the certificate server. To disable the CRL checking, simply delete the **StrongCRLCheck** value under the **Oakley** key and restart the service or reboot.

UNDERSTANDING IKE NEGOTIATION (ADVANCED USERS)

This section is provided for those who want to learn more about the details of IKE negotiation behavior, and is not required to complete the walkthrough. Detailed explanations of IPSec, IKE and other aspects of the implementation are available in the online help for both Windows 2000 Server and Professional versions. Simply start the IPSec Policy Management snap-in and choose Help. In some cases, references to ISAKMP/Oakley may be seen. This was the former name of the Internet Key Exchange specification, and the references to it appear as artifacts of the beta version.

Failure and Success of IKE, along with a reason for the failure, are events audited in the Security event log. The procedure for enabling auditing is given at the start of this walkthrough. If the server is using Server policy, and falls back to clear for destinations that do not reply to the IKE request, this is tracked by an audit event for what is called a *soft security association*. This appears in the IPSec monitor as having a negotiation policy of <none>. If the server is using Secure Server and gives up trying to reach a destination, with no IKE response from that destination, it will not be audited.

You can use the Server policy and the audit log on a server to discover and track the destinations that the server communicates with over time. Thus, you can better understand how to build a custom policy that will secure the right applications and client communication, while permitting other maintenance and infrastructure communication to go unprotected in the clear.

The initial long form of the IKE negotiation (main mode) performs the authentication and establishes an IKE security association (SA) between machines, which involves generating the master key material. Once successful, default settings in the default policies (see Key Exchange on the policy's General Tab) will make the IKE SA last for 8 hours. If data is actively being transferred at the end of the 8 hours, then the main mode security association will be renegotiated automatically.

The shorter version of IKE negotiation (quick mode) occurs after main mode to establish an IPSec security association to secure particular traffic according to the packet filters in the policy's rules. The IPSec SA negotiation involves choosing algorithms, generating session keys, and determining the Security Parameter Index (SPI) numbers used in the packets. The IPSec monitor shows only these IPSec security associations. After five minutes of idle time, the IPSec security association is cleaned up, and will disappear from the IPSec monitor display. If traffic is sent again that requires the IPSec security association, then an IKE quick mode negotiation occurs to re-establish the IPSec security association, using new keys and SPIs. The default values set in the default security methods require a new IPSec security association every 15 minutes (900 seconds) or after 2 gigabytes have been transferred. If data is actively being transferred, then the IPSec security associations will be automatically renegotiated.

Troubleshooting Policy Configuration

This walkthrough is intended to cover only local computer IPSec policy that uses IPSec transport (not tunneling) to secure traffic between a source computer and a destination computer. It does not to cover using Group Policy in the Active Directory to distribute IPSec policy. IPSec policy configuration is very flexible and thus very powerful. There are a number of security configuration issues that you will want to be aware of. Please read the Release Notes. Then read the additional notes below to help clarify what is not supported in policy configurations by design. If you are not able to get any IPSec communication to work, then follow the steps provided below to build the simplest policy, and use it for testing.

Only One Authentication Method Between a Pair of Hosts

IPSec policy is designed so that only one authentication method can be used between a single pair of hosts, regardless of how many are configured. If you have multiple rules that apply to the same pair of computers, you must make certain those rules allow that pair of computers to use the same authentication method. You must also validate all credentials used for that authentication method. For example, the IPSec snap-in allows you to configure policy between two hosts that use Kerberos to authenticate TCP data, and use certificates to authenticate UDP data. However, this policy does not work correctly, because it uses two different authentication methods between a single pair of hosts.

One-Way IPSec Protection of Traffic Not Allowed

IPSec policy is designed so that rules specifying one-way protection of traffic by IPSec will not work. If you create a policy to protect traffic between hosts A and B, then you must specify both traffic from A to B and traffic from B to A in the filter. You can do this by creating two filters in the same filter list. Or you can go to the Filter Specification Properties dialog box in the IPSec snap-in and select the Mirrored box. This option is selected by default, because protection must be negotiated for both directions, even if the data traffic itself only flows one way.

You can create one-way filters to block or permit traffic, but not to secure traffic. To secure traffic, you have to specify the filter mirror or have the system generate it.

Computer Certificates Must Have Private Key

Incorrectly obtained certificates may result in a condition in which the certificate exists, and is chosen to be used for IKE authentication, but fails to work because the private key corresponding to the certificate's public key is not present on the local computer.

To verify that the Certificate has a private key

1. On the **Start** menu, click **Run**, and then type **mmc** and Click **OK**.
2. On the **Console** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. In the **Snap-in** list, double-click **Certificates**. Click **Close**, and then click **OK**.
4. Double-click **Certificates-User (local computer**), and then double-click **Personal**.

5. In the details pane, double-click the **Certificates** folder.

6. Double-click the certificate you want to check.

On the General tab, you must see the text**, You have a private key that corresponds to this certificate**, for the system to use this certificate successfully for IPSec.

Depending upon how the certificate was requested and populated into the host's local certificate store, this private key value may not exist, or may not be available to be used during the IKE negotiation. If the certificate in the personal folder does not have a corresponding private key, then certificate enrollment has failed. If a certificate was obtained from the Microsoft Certificate Server with the option set for *strong private key protection*, the user must enter a PIN number to access the private key each time that the private key is used to sign data in the IKE negotiation. Because the IKE negotiation is being done in the background by a system service, there is no window available to the service to prompt the user. So certificates obtained with this option will not work for IKE authentication.

Build and Test the Simplest End-to-End Policy

Most problems, particularly interoperability problems, can be resolved by creating the simplest policy rather than by using the default policies. When you create a new policy, do not enable an IPSec tunnel, or the default response rule. Edit the policy on the general tab, edit the key exchange to have only one option that the destination will accept, perhaps the RFC MUST options of DES, SHA1, with group 1 Diffie Hellman. Create a filter list with one mirrored filter that specifies source "My IP Address" and destination of only the destination IP address that you are trying to communicate securely with. Choose protocol ICMP. We recommend testing by creating a filter only for ICMP or pinging traffic between your computer and the other computer. Create your own filter action to negotiate security using only one security method. If you want to see the traffic in the IPSec formatted packets with a network monitor, use Medium Security (AH format), otherwise choose custom, and build one single security method, perhaps an RFC MUST set of parameters such as format ESP using DES with SHA1, with no lifetimes specified. Make sure both check boxes are cleared in the security method, so that it requires IPSec for the destination, and will not communicate with non-IPSec computers, and does not accept unsecured communications. Use an authentication method of pre-shared key for the rule, and make sure there are no whites paces in the string of characters. The destination must use exactly the same pre-shared key.

Note The same configuration must be configured on the destination also, only the IP addresses are different for source and destination.

You should assign this simple policy active on a computer, then ping from that computer to the destination. You should see ping return "Negotiating security." This indicates that the policy's filter is being matched and that IKE should be trying to negotiate security with the destination for the ping packet. If you continue to see **Negotiating IP Security** from multiple tries to ping the destination, then you

probably do not have a policy problem; rather, you may have an IKE problem. See the “Troubleshooting IKE Negotiation” section below.

Using The IPSec Policy Tracing (Expert Users)

As a last resort, you may wish to study the IPSec Policy Agent trace log which shows the policy that it gives to the other IPSec components, as well as reactions to plug and play events. See %windir%\ipsecpa.log. This log file format may change and may be disabled by default in the final product.

Troubleshooting IKE Negotiation

Clearing IKE State

To completely clear the state of IKE negotiation, it is necessary to stop and start the policy agent service using the commands below from a command shell prompt when logged in as an administrator:

```
net stop policyagent
net start policyagent
```

Retry your steps to secure traffic.

Using the Security log To See IKE Errors

The Security event log records the reason for failure when an IKE negotiation fails. Use these messages to detect that a negotiation failed and why. You must enable auditing using the procedure at the start of this walkthrough.

Using A Network Sniffer or Monitor

If none of the above has helped, and you have not read the section, “Understanding IKE Negotiation,” please do so now.

For more detailed investigations, use a network monitor, such as Netmon, to sniff the packets being exchanged. Remember that most of the content of the packets used in IKE negotiation is encrypted and cannot be interpreted by a network sniffer. Still, it may be worthwhile to sniff all traffic to and from the computer to be sure that you see the traffic you are expected to see. A limited version of Netmon is provided in every Windows 2000 Server. It is not installed by default, so you must go into **Add/Remove Software**, **Windows Components**, **Networking**, then select the **Network Monitor**, and follow the steps required.

Using IKE Tracing (Expert Users)

For experts in IKE negotiation, the tracing option for IKE negotiation is shipped in Beta 3 as enabled. See %windir%\Oakley.log. This file is size limited, and will be started new when the PolicyAgent service is started. This log file format may change and may be disabled by default in the final product.

FOR MORE INFORMATION

For the latest information on Microsoft Windows 2000 network operating system, visit our World Wide Web site at http://www.microsoft.com/windows/server/ and the Windows NT Server Forum on the Microsoft Network (GO WORD: MSNTS).

For the latest information on the Windows 2000 Beta 3, visit the World Wide Web site at http://ntbeta.microsoft.com.

For information about default security settings in Windows 2000, see the white paper at http://www.microsoft.com/windows/server/Technical/security/.

Before You Call for Support

Please keep in mind that Microsoft does not support these walkthroughs. The purpose of the walkthroughs is to facilitate your initial evaluation of the Microsoft Windows 2000 features. For this reason, Microsoft cannot respond to questions you might have regarding specific steps and instructions.

Reporting Problems

Problems with Microsoft Windows 2000 Beta 3 should be reported via the appropriate bug reporting channel and alias. Please make sure to adequately describe the problem so that the testers and developers can reproduce it and fix it using the procedures below. Refer to the Release Notes included on the Windows 2000 Beta 3 distribution media for some of the known issues.

Customers who are members of the Technical Beta Sites program can use newsgroup: ms.beta.win2000.networking

General Beta3 participants can subscribe to the public newsgroup: microsoft.public.win2000.beta.networking

If you have questions specific to certificate usage or Kerberos authentication or other general security feature, then use the security newsgroup instead. If you do report a problem, first describe your problem in a message posted to the appropriate Windows 2000 beta news group that includes

Title of Problem (25 words or less) including the bug number if already filed

1. Description of computers on which the problem is observed, including what network cards and operating system build number
2. Description of what you are trying to do
3. Description of how you configured policy on both sides. We will not be able to help you if you are not specific about the policy configuration on each side of communication
4. Description of what happened, the observed problem
5. Description of the local network or path over which the communication is taking place between the two computers

Before changing the configuration on either computer, save the logs noted below in

case detailed investigation is required. The Windows 2000 beta support engineer may then require additional information below:

1. Attach a copy of the output “ipconfig /all” output.
2. Attach a copy of output for “route print.”
3. Attach a sniff of the Ethernet (not just IP) traffic to and from the affected computer during the time that you discovered or reproduced the problem.
4. Attach the %windir%\ipsecpa.* log files: ipsecpa.log, ipsecpa.log.last, ipsecpa.bak and ipsecpa.bak.last.
5. Attach the %windir%\oakley.* files: oakley.log, oakley.log.sav, oakley.log.bak.sav.